R mot control syst m for motor vehicle r lated d vices

Patent Number: US5940007

Publication date: 1999-08-17

Inventor(s): SCHWEGLER GUENTER (DE); HIPP ARTHUR (DE); HOFFMANN DANIEL (DE); WEIGAND DIRK (DE); BRINKMEYER HORST (DE)

Applicant(s): DAIMLER BENZ AG (DE)

Requested Patent: DE19607017

Application Number: US19970804884 19970224

Priority Number(s): DE19961007017 19960224

IPC Classification: G06F7/04; G08C19/00; H02H7/18

EC Classification: B60R25/00, G07C9/00B2, H04L9/32B, G07C9/00E4, G07C9/00E16

Equivalents:

Abstract

A system and method for operating a remote control having a portable remote control unit which can control at least one function unit. The remote control unit and the function unit are connected with one another by way of a bidirectional data communication link, by which data can be transmitted by means of a symmetrical coding method. The remote control unit sends a learn mode reporting signal in a secret coding information learn mode to the controllable function unit which, in the learn mode, in turn, sends back an acknowledgment signal. Upon receipt of the acknowledgment signal, the remote control unit generates new secret coding information by means of the coding algorithm, as a function of basis secret coding information and of the previous secret coding information, and sends the new secret coding information to the function unit. The function unit then replaces the previous secret coding information with the new secret coding information and emits an acknowledgment signal, upon the receipt of which the remote control unit, in turn, replaces the previous secret coding information with the new secret coding information.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Patentschrift**

(10) **DE 196 07 017 C 2**

(51) Int. Cl.[7]:
H 04 Q 9/00
H 04 L 9/12
B 60 R 25/00
H 02 J 13/00
G 07 C 11/00

(21) Aktenzeichen: 196 07 017.1-32
(22) Anmeldetag: 24. 2. 1996
(43) Offenlegungstag: 28. 8. 1997
(45) Veröffentlichungstag der Patenterteilung: 29. 6. 2000

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
DaimlerChrysler AG, 70567 Stuttgart, DE

(72) Erfinder:
Brinkmeyer, Horst, Dr.-Ing., 71336 Waiblingen, DE; Hipp, Arthur, 73230 Kirchheim, DE; Hoffmann, Daniel, 73733 Esslingen, DE; Schwegler, Günter, 71384 Weinstadt, DE; Weigand, Dirk, 04207 Leipzig, DE

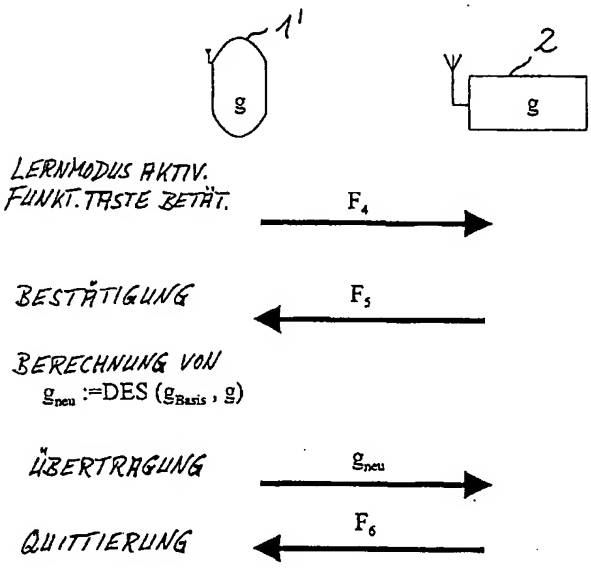
(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

DE	44 11 450 C1
DE	42 15 221 C2
DE	40 18 261 C1
DE	30 43 627 C2
DE	41 02 020 A1
DE	40 03 280 A1
DE	32 25 754 A1
US	49 88 992
EP	06 17 183 A2
WO	90 15 211 A1

(54) Fernbedienungseinrichtung und Betriebsverfahren hierfür, insbesondere zur Ansteuerung von kraftfahrzeugbezogenen Einrichtungen

(57) Fernbedienungseinrichtung, insbesondere zur Steuerung von kraftfahrzeugbezogenen Einrichtungen, mit
- einer tragbaren Fernbedieneinheit (1),
- wenigstens einer über die Fernbedieneinheit ansteuerbaren Funktionseinheit (2) und
- einer bidirektionalen Datenkommunikationsstrecke (17), über die mittels eines symmetrischen Verschlüsselungsverfahrens codierte Daten zwischen der Fernbedieneinheit und der Funktionseinheit übertragbar sind,

dadurch gekennzeichnet, daß
- die Fernbedieneinheit (1) bei Aktivierung eines Verschlüsselungsgeheimnis-Lernmodus ein Lernmodus-Meldesignal (F_4) abgibt,
- die Funktionseinheit (2) im Lernmodus auf den Empfang des Lernmodus-Meldesignals (F_4) hin ein Lernmodus-Bestätigungssignal (F_5) abgibt,
- die Fernbedieneinheit auf Empfang des Lernmodus-Bestätigungssignals hin mittels des Verschlüsselungsalgorithmus des symmetrischen Verschlüsselungsverfahrens in Abhängigkeit eines bisherigen Verschlüsselungsgeheimnisses (g) ein neues Verschlüsselungsgeheimnis (g_{neu}) ermittelt und an die Funktionseinheit sendet,
- die Funktionseinheit nach Empfang des neuen Verschlüsselungsgeheimnisses (g_{neu}) das bisherige Verschlüsselungsgeheimnis (g) durch das neue ersetzt und ein Quittierungssignal (F_6) an die Fernbedieneinheit sendet und
- die Fernbedieneinheit auf Empfang des Quittierungssignals hin das bisherige Verschlüsselungsgeheimnis (g) durch das neue Verschlüsselungsgeheimnis (g_{neu}) ersetzt.



DE 196 07 017 C 2

DE 196 07 017 C 2

Beschreibung

Die Erfindung bezieht sich auf eine Fernbedienungseinrichtung mit einer tragbaren Fernbedieneinheit, wenigstens einer über die Fernbedieneinheit ansteuerbaren Funktionseinheit und einer bidirektionalen Datenkommunikationsstrecke, über welche mittels eines symmetrischen Verschlüsselungsverfahrens codierte Daten zwischen der Fernbedieneinheit und der Funktionseinheit übertragbar sind, sowie auf ein Betriebsverfahren für eine solche Einrichtung.

Fernbedienungseinrichtungen dieser Art dienen beispielsweise dazu, den Zugang oder die Nutzungsberechtigung eines Kraftfahrzeuges oder die Steuerung externer kraftfahrzeugbezogener Vorrichtungen, wie eines Garagentoröffners, codegeschützt nur einem ausgewählten Kreis von berechtigten Nutzern zu erlauben. Die berechtigten Nutzer weisen der jeweiligen ansteuerbaren Funktionseinheit ihre Nutzungsberechtigung dadurch nach, daß sie im Besitz einer berechtigenden Fernbedieneinheit sind und über diese einen bidirektionalen Codedatenaustausch mit der Funktionseinheit auslösen, innerhalb welchem der zugehörige Berechtigungscode verschlüsselt zwischen den beiden Einheiten übertragen und anschließend auf Übereinstimmung und damit Nutzungsberechtigung geprüft wird. Die Verwendung eines symmetrischen Verschlüsselungsverfahrens, welches das Vorhandensein eines identischen Verschlüsselungsgeheimnisses in beiden Einheiten voraussetzt, bietet einen hohen Schutz vor Versuchen durch Unberechtigte, mittels Abhören eines derartigen Codedatenaustauschs anschließend selbst erfolgreich die Funktionseinheit ansteuern zu können.

In der Offenlegungsschrift DE 32 25 754 A1 sind eine Fernbedienungseinrichtung der eingangs genannten Art sowie ein Betriebsverfahren hierfür offenbart, bei dem das Verschlüsselungsgeheimnis des verwendeten symmetrischen Verschlüsselungsverfahrens eine mathematische Funktion ist, die identisch und unveränderbar einerseits in einem Schlüsselteil und andererseits in einem Schloßteil abgelegt ist.

In der Kryptographie ist unter anderem der sogenannte DES(Data Encription Standard)-Algorithmus als ein hochsicherer Algorithmus für symmetrische Verschlüsselungsverfahren bekannt, der beispielsweise in einer in der Patentschrift DE 44 11 450 C1 beschriebenen Fahrzeugsicherungseinrichtung mit elektronischer Nutzungsberechtigungscodierung zur Ersatzschlüsselimplementierung anstelle eines dort ansonsten für einen geschützten Codedatenaustausch verwendeten asymmetrischen Verschlüsselungsverfahrens, bei dem nur einer der beiden miteinander kommunizierenden Einheiten ein Verschlüsselungsgeheimnis zu enthalten braucht, vorgeschlagen wird.

Es ist verschiedentlich bekannt, eine tragbare Fernbedieneinheit in Form eines elektronischen Fahrzeugschlüssels, der zum Zugang und/oder zur Nutzung eines Kraftfahrzeuges berechtigt, zusätzlich zur Ansteuerung weiterer Fahrzeugfunktionseinheiten oder sonstiger Funktionseinheiten, wie eines Garagentoröffners, zu verwenden, wozu stellvertretend auf die Patentschriften DE 30 43 627 C2, DE 40 18 261 C1 und DE 42 15 221 C2 sowie die Offenlegungsschrift DE 40 03 280 A1 hingewiesen sei.

In der Offenlegungsschrift DE 41 02 020 A1 ist eine Fernbedienungseinrichtung mit einem Fahrzeugschlüssel beschrieben, der für bidirektionalen Informationsaustausch mit dem Fahrzeug zwecks Ansteuerung von Verriegelungs- und Entriegelungsorganen desselben eingerichtet ist und außerdem eine optische Anzeigeeinheit aufweist, auf der vom Fahrzeug übertragene Informationen bezüglich Fahrzustandsparameter, wie Zustand der Fahrzeugtüren, gefahrene Kilometerstrecke, Füllstand im Kraftstofftank, sowie ggf. bezüglich weiterer Parameter, wie Uhrzeit und Zustand der Batterie des Schlüssels, optisch angezeigt werden können.

Aus der Offenlegungsschrift EP 0 617 183 A2 ist eine Fernbedienungseinrichtung mit einem Schlüssel für ein Kraftfahrzeug bekannt, der einen Sprachspeicher, ein Mikrofon und eine Sprachwiedergabeeinheit enthält. In den so ausgelegten Schlüssel können Informationen, wie beispielsweise die Nummer eines Parkplatzes, auf dem sich das Fahrzeug befindet, in Sprachform eingegeben und dort abgespeichert werden, wonach diese Informationen auf Anforderung durch den Benutzer wieder aus dem Schlüssel in Sprachform ausgegeben werden können.

In der Offenlegungsschrift WO 90/15211 ist eine Fernbedienungseinrichtung der eingangs genannten Art beschrieben, bei der Daten zwischen der Fernbedieneinheit und der Funktionseinheit übertragbar sind, die eine beispielsweise durch das DES-Verschlüsselungsverfahren kodierte Zufallszahl beinhalten. Das zugehörige Verschlüsselungsgeheimnis kann in der Fernbedieneinheit dadurch geändert werden, daß letztere mit einer zusätzlichen Kodiereinheit zusammengebracht wird, über die der Benutzer zunächst zum Nachweis seiner Berechtigung das bisherige Verschlüsselungsgeheimnis einzugeben hat. Verläuft die zugehörige Codeübereinstimmungsprüfung erfolgreich, kann der Benutzer über die Kodiereinheit ein neues Verschlüsselungsgeheimnis in die Fernbedieneinheit einspeisen. Die Übertragung des neuen Verschlüsselungsgeheimnisses in die Funktionseinheit erfolgt im Anschluß an einen normalen Authentikationsvorgang, der wegen des bislang nur in der Fernbedieneinheit geänderten Verschlüsselungsgeheimnisses negativ verläuft. Die Funktionseinheit versetzt sich dann in einen Lernmodus und ruft über das DES-Verschlüsselungsverfahren das neue Verschlüsselungsgeheimnis von der Fernbedieneinheit ab.

Bei einer in der Patentschrift US 4.988.992 beschriebenen Fernbedienungseinrichtung sind Autorisierungscodes von wenigstens einer Fernbedieneinheit zu wenigstens einer Funktionseinheit übertragbar. Dabei kann der jeweils verwendete Autorisierungscode bei Bedarf geändert werden. Dazu wird zuerst die betreffende Fernbedieneinheit in einen Programmiermodus gebracht, was einen dort vorzusehenden Zufallscodegenerator aktiviert. Der von diesem erzeugte Zufallscode wird als neuer Autorisierungscode in der Fernbedieneinheit gespeichert. Gegebenenfalls weitere vorgesehene Fernbedieneinheiten können durch Aktivieren eines Lernmodus synchronisiert werden, in welchem sie über eine spezielle Antenne den neuen Autorisierungscode von der neu programmierten Fernbedieneinheit empfangen können, wenn letztere in unmittelbare Nähe gebracht und zum Senden des neuen Autorisierungscodes veranlaßt wird. Zum Einbringen des neuen Autorisierungscodes in die jeweilige Funktionseinheit wird an derselben ein Programmiermodus aktiviert, woraufhin diese für eine vorgegebene Zeitdauer zum Empfang eines neuen, nicht mit ihrem bisher gespeicherten Code übereinstimmenden Autorisierungscodes bereit ist. Ein ggf. innerhalb dieser Zeitspanne empfangener Code wird dann von der Funktionseinheit als neuer Autorisierungscode gespeichert.

Der Erfindung liegt als technisches Problem die Bereitstellung einer Fernbedienungseinrichtung der eingangs genannten Art sowie eines hierfür geeigneten Betriebsverfahrens zugrunde, bei denen mit relativ geringem Aufwand dafür gesorgt ist, daß das für das verwendete symmetrische Verschlüsselungsverfahren benutzte Verschlüsselungsgeheimnis in einfacher und manipulationsgeschützter Weise verändert werden kann.

Dieses Problem wird durch eine Fernbedienungseinrichtung mit den Merkmalen des Anspruchs 1 sowie ein Verfahren mit den Merkmalen des Anspruchs 6 gelöst. Der von

dieser Einrichtung bzw. diesem Verfahren realisierbare Lernvorgang zur Ersetzung eines bisherigen Verschlüsselungsgeheimnisses durch ein neues zeichnet sich sowohl durch hohe Manipulationssicherheit als auch durch gleichzeitig einfache Handhabbarkeit aus. Die Fernbedieneinheit berechnet bei Aktivierung des Lernmodus selbsttätig ein neues Verschlüsselungsgeheimnis, vorzugsweise nach einem Pseudozufallsverfahren. Da das Verschlüsselungsgeheimnis selbst für den rechtmäßigen Besitzer der Fernbedieneinheit verborgen bleibt, wird dieser nicht mit der Eingabe eines Verschlüsselungsgeheimnisses belastet. Aufgrund der Generierung eines jeweils neuen Verschlüsselungsgeheimnisses auf Anforderung ist der Lernmodus zwecks Wahl eines neuen Verschlüsselungsgeheimnisses beliebig oft wiederholbar. Mit den Maßnahmen des Bestätigens einer Lernaktivierung und des Quittierens einer Verschlüsselungsgeheimnisänderung durch die Funktionseinheit an die Fernbedieneinheit und der erst daraufhin in der Funktionseinheit erfolgenden Verschlüsselungsgeheimnissetzung ist sichergestellt, daß ein von einem Unberechtigten ausgelöstes Erzeugen eines neuen Geheimnisses zum einen für diesen wertlos bleibt, da die Funktionseinheit weiterhin mit dem alten Verschlüsselungsgeheimnis anzusteuern ist, und zum anderen der berechtigte Benutzer die Funktionseinheit weiterhin mit der Fernbedieneinheit auf der Basis des weiter geltenden Verschlüsselungsgeheimnisses anzusteuern vermag. Alternativ dazu ist es möglich, die Erzeugung eines neuen Verschlüsselungsgeheimnisses in der Fernbedieneinheit bei nicht aktivierter Funktionseinheit erst gar nicht zuzulassen. Die Funktionseinheit sollte zweckmäßigerweise vor dem Zugriff Unberechtigter bewahrt und die Aktivierung des Lernmodus bei der Funktionseinheit durch eine geeignete Verriegelung, wie beispielsweise einen Schlüsselschalter, geschützt werden.

Mit einer nach Anspruch 2 weitergebildeten Fernbedienungseinrichtung können über die Fernbedieneinheit sowohl mindestens eine fahrzeugseitige Funktionseinheit, z. B. eine Standheizung, als auch mindestens eine fahrzeugexterne Funktionseinheit, z. B. ein Garagentoröffner, angesteuert werden. Darüber hinaus können in umgekehrter Datenübertragungsrichtung Zustandsinformationen, insbesondere bezüglich der jeweiligen Funktionseinheit, an die Fernbedieneinheit übermittelt und dort optisch und/oder akustisch zur Anzeige gebracht werden.

Bei einer nach Anspruch 3 weitergebildeten Einrichtung und einem nach Anspruch 7 weitergebildeten Verfahren ist jeder der von der Fernbedieneinheit ansteuerbaren Funktionseinheiten ein eigenes Verschlüsselungsgeheimnis für den Verschlüsselungsalgorithmus in der Fernbedieneinheit zugeordnet, so daß die Verschlüsselungsgeheimnisse für verschiedene ansteuerbare Funktionseinheiten unabhängig voneinander geändert werden können.

Bei einer nach Anspruch 4 weitergebildeten Einrichtung und einem nach Anspruch 8 weiterbildeten Verfahren beinhaltet die ansteuerbare Funktionseinheit eine Auswahlmöglichkeit zwischen mehreren Lernmodus-Kanälen, von denen jeder zum Setzen eines Verschlüsselungsgeheimnisses zur Datenkommunikation mit einer bestimmten Fernbedieneinheit dient. Auf diese Weise kann die Funktionseinheit von mehreren berechtigenden Fernbedieneinheiten mit jeweils spezifischem Verschlüsselungsgeheimnis angesteuert werden.

Eine besonders sichere Datenkommunikation zwischen Fernbedieneinheit und ansteuerbarer Funktionseinheit bei vertretbar geringem Aufwand ermöglichen eine nach Anspruch 5 weitergebildete Einrichtung und ein nach Anspruch 9 weitergebildes Verfahren, in welchen der sogenannte DES(Data Enscription Standard)-Algorithmus für das symmetrische Verschlüsselungsverfahren verwendet wird.

Bevorzugte Ausführungsformen der Erfindung sind in den Zeichnungen dargestellt und werden nachfolgend beschrieben. Hierbei zeigen:

Fig. 1 ein Blockdiagramm einer Fernbedienungseinrichtung zur Steuerung von kraftfahrzeuginternen und kraftfahrzeugexternen Einrichtungen über eine tragbare Fernbedieneinheit in Form eines Schlüsselanhängers,

Fig. 2 eine schematische Rückansicht des Schlüsselanhängers von **Fig.** 1,

Fig. 3 eine Darstellung eines Authentikationskommunikationsvorgangs mit der Einrichtung von **Fig.** 1 zwischen Schlüsselanhänger und einem Garagentoröffner,

Fig. 4 eine Darstellung der Bedienschritte eines Verschlüsselungsgeheimnis-Lernvorgangs zwischen einem modifizierten Schlüsselanhänger als tragbarer Fernbedieneinheit und dem Garagentoröffner der Einrichtung von **Fig.** 1 und

Fig. 5 eine Darstellung des Kommunikationsablaufs während des Lernvorgangs gemäß **Fig.** 4.

Fig. 1 zeigt im Überblick als Blockdiagramm eine Fernbedienungseinrichtung, bei der eine tragbare Fernbedieneinheit in Form eines Schlüsselanhängers (**1**) vorgesehen ist, der über eine bidirektionale Datenkommunikationsstrecke (**17**), speziell einer Funkstrecke mit drei Funkkanälen (Fu1, Fu2, Fu3), je nach Betätigung zugehöriger Funktionstasten mit einer Sende-/Empfangseinrichtung (**2a**) eines einer Fahrzeuggarage zugeordneten Garagentoröffners (**2**), mit einer Sende-/Empfangseinrichtung (**3a**) eines Wohnhauses (**3**) oder mit einer Sende-/Empfangseinrichtung (**4a**) eines Fahrzeuges (**4**) in Datenaustauschverbindung treten kann, und zwar jeweils über einen zugehörigen der drei Funkkanäle (Fu1, Fu2, Fu3). Der Schlüsselanhänger (**1**) vermag die fahrzeugexternen Einrichtungen auch dann über die zugehörigen Funkkanäle (Fu1, Fu2) anzusteuern, wenn er sich im Fahrzeuginnenraum befindet, wie durch die gezeigte Position (**1a**) angedeutet. Dabei erfolgt die zugehörige Datenkommunikation vollständig unabhängig vom Fahrzeug (**4**) und dessen Sende-/Empfangseinrichtung (**4a**). Zur Verbesserung der Übertragungseigenschaften ist es optional dazu auch möglich, eine Umsetzung der Signale des Schlüsselanhängers (**1a**) auf die Sende-/Empfangseinrichtung (**4a**) des Fahrzeuges vorzunehmen. Diese wickelt dann die Kommunikation mit der dem Garagentoröffner zugeordneten Sende-/Empfangseinrichtung über einen in **Fig.** 1 strichpunktiert angedeuteten, optionalen Funkkanal ($Fu1_{opt}$) ab. Selbstverständlich kann bei Bedarf auch eine andere drahtlose Datenkommunikationsstrecke, z. B. auf der Basis von Infrarotwellen, verwendet werden.

Die Sende-/Empfangseinrichtung (**2a**) des Garagentoröffners (**2**) besitzt einen Schaltausgang, der parallel zu einem hier nicht weiter gezeigten Bedienelement im Innenraum der Garage einen Garagentorstellantrieb (**2b**) ansteuert, so daß das Garagentor wahlweise über den Schlüsselanhänger (**1**) oder das Bedienelement im Garageninnenraum motorisch geöffnet und geschlossen werden kann. Die Sende-/Empfangseinrichtung (**3a**) im Wohnhaus (**3**) steuert mit einem Schaltausgang einen elektromechanischen Türöffner (**3b**) an, welcher der Haustüre des Wohnhauses (**3**) zugeordnet ist. Damit kann über den Schlüsselanhänger (**1**) das Öffnen der Haustür freigegeben oder gesperrt werden. Es versteht sich, daß die beiden Sende-/Empfangseinrichtungen (**2a, 3a**) von Garagentoröffner (**2**) und Wohnhaus (**3**) bei Bedarf auch zu einer einteiligen, mehrkanaligen Sende-/Empfangseinrichtung vereint sein können. Die Sende-/Empfangseinrichtung (**4a**) im Fahrzeug (**4**) ist mit den anderen Komponenten der fahrzeugelektrischen Anlage über ein

nicht gezeigtes Datenbussystem verbunden.

Der als tragbare Fernbedieneinheit fungierende Schlüsselanhänger (1) besitzt, wie aus der Vorderansicht von **Fig. 1** und der Rückansicht von **Fig. 2** hervorgeht, mehrere Funktionalitäten. Über eine Funktionstaste (5) an der Vorderseite erfolgt die Auslösung eines Datenkommunikationsvorgangs zur Ansteuerung des Garagentoröffners (2) und über eine weitere Funktionstaste (6) die Ansteuerung des Haustüröffners (3b). Einer dritten Funktionstaste (7) kann eine frei wählbare Funkfernbedienfunktion hinterlegt werden, wozu vorher ein geeignetes Datenprotokoll eingegeben wird. Eine mögliche Funktion ist diejenige des Einschaltens eines Hoflichtes. In einer Alternativlösung kann ein solches Hoflicht auch über einen weiteren, zugeordneten Kommunikationskanal in der Sende-/Empfangseinrichtung (2a) des Garagentoröffners (2) erfolgen. Bei dieser Variante braucht dann kein eigenes Funkdatenprotokoll eingespeist werden.

Der Schlüsselanhänger (1) besitzt des weiteren ein Display (8), das über eine Beleuchtungstaste (9) beleuchtet werden kann. Auf dem Display (8) ist bei Betätigen einer Menütaste (10) ein Menü mit zuvor abgelegten, fahrzeuginternen Funktionalitäten darstellbar, aus dem durch Betätigen einer Setztaste (11) eine jeweils gewünschte Funktionalität ausgewählt werden kann. Im gezeigten Beispiel von **Fig. 1** ist als eine solche Funktionalität die Ansteuerung der Standheizung durch ein entsprechendes Symbol (16), das auf dem Display (8) erscheint, repräsentiert. Die Ansteuerung der aus dem Menü ausgewählten fahrzeuginternen Funktionalitäten erfolgt über den Funkkanal (Fu3) zwischen Schlüsselanhänger (1) und Fahrzeug (4), wobei die fahrzeugseitige Sende-/Empfangseinrichtung (4a) die entsprechenden Steuerbefehle über das Datenbussystem an die jeweilige Fahrzeugzielkomponente weiterleitet.

An seiner Rückseite weist der Schlüsselanhänger (1), wie aus **Fig. 2** ersichtlich, eine Funktionstaste (12), die der Auswahl eines Lernmodus dient und weiter unten näher erläutert wird, sowie eine Funktionstaste (13), die als sogenannter Paniktaster dient, auf, wobei beide Funktionstasten (12, 13) vor unabsichtlicher Betätigung dadurch geschützt sind, daß sie versenkt angeordnet sind oder alternativ einen vergleichsweise harten Druckpunkt besitzen. Durch Betätigen des Paniktasters (13) kann eine im Fahrzeug vorhandene Alarmanlage ausgelöst werden. Gegebenenfalls ist es des weiteren im Zusammenwirken der Fahrzeugdiebstahlwarnanlage mit einem Autotelefon und einem Ortungssystem, wie dem GPS (Global Positioning System), möglich, einen Notruf abzusetzen. Des weiteren sind an der Rückseite des Schlüsselanhängers (1) ein Lautsprecher (14) und ein Mikrofon (15) angeordnet, mit denen eine Sprachaufzeichnung und -wiedergabe möglich ist. Speziell können beispielsweise Informationen über den Fahrzeugstandort in Sprachform eingegeben und später wieder abgerufen werden. Diese Funktion eignet sich insbesondere bei Mehrfachnutzung des zugehörigen Fahrzeuges (4) in einem Fuhrpark. Zusätzlich kann vorgesehen sein, Zustandsinformationen der vom Schlüsselanhänger (1) angesteuerten Funktionselemente, wie des Garagentoröffners (2), des Haustüröffners (3b) und der Fahrzeug-Standheizung oder auch andere Informationen, die dem Schlüsselanhänger (1) über die mit ihm verbundenen Sende-/Empfangseinrichtungen (2a, 3a, 4a) und die bidirektionale Datenkommunikationsstrecke (17) übermittelt werden, auf dessen Display (8) optisch anzuzeigen. So können beispielsweise auch Fahrzeugdaten wie Kilometerstand und Tankinhalt auf dem Display (8) angezeigt werden, was wiederum insbesondere bei Mehrfachnutzung des Fahrzeugs durch mehrere Fahrzeugführer, wie bei Autovermietungen und sogenannten Car-Sharing-Pools, von besonderem Nutzen ist. Ebenso kann auf diese Weise bei Bedarf der Verriegelungszustand der Fahrzeugtüren über die fahrzeugseitige Sende-/Empfangseinrichtung (4a) und den zugehörigen Funkkanal (Fu3) an den Schlüsselanhänger (1) übermittelt und dort auf dem Display (8) angezeigt werden.

Als weitere vorteilhafte Funktionalität der Fernbedienungseinrichtung kann vorgesehen sein, daß bei Auslösung der Fahrzeugdiebstahlwarnanlage aufgrund eines Diebstahlversuchs ein entsprechendes Informationssignal von der Sende-/Empfangseinrichtung (4a) des Fahrzeugs (4) über den zugehörigen Funkkanal (Fu3) zum Schlüsselanhänger (1) übermittelt wird und dieser daraufhin eine entsprechende Meldung über den Diebstahlversuch auf seinem Display (8) optisch und/oder über seinen Lautsprecher (14) akustisch abgibt.

Um einen Mißbrauch der Fernbedienungseinrichtung durch Unberechtigte zu verhindern, ist die Datenkommunikation zwischen dem Schlüsselanhänger (1) einerseits und den mit ihr in Verbindung stehenden Sende-/Empfangseinrichtungen (2a, 3a, 4a) durch eine Nutzungsberechtigungsprüfung geschützt, deren erfolgreicher Ablauf Voraussetzung dafür ist, daß ein gesendetes Datensignal, insbesondere ein jeweiliges Ansteuersignal für den Garagentüröffner (2), den Haustüröffner (3b) oder die Fahrzeugstandheizung, nach Aussenden ordnungsgemäß empfangen bzw. weiterverarbeitet wird. Für einen solchen Authentikationsvorgang, mit dem die Berechtigung des jeweils betätigten Schlüsselanhängers (1) zur Ansteuerung der gewünschten Funktionseinheit geprüft wird, kommt in der Fernbedienungseinrichtung von **Fig. 1** ein symmetrisches Verschlüsselungsverfahren zum Einsatz, das den sogenannten DES(Data Encription Standard)-Algorithmus benutzt. Die Sicherheit des DES-Algorithmus beruht nicht auf der Geheimhaltung des Algorithmus an sich, sondern auf derjenigen eines im Verschlüsselungsalgorithmus verwendeten Verschlüsselungsgeheimnisses (g), das einerseits im Schlüsselanhänger (1) und andererseits in den Sende-/Empfangseinrichtungen (2a, 3a, 4a) der angesteuerten Funktionseinheiten abgelegt ist. Dabei erzeugt der Verschlüsselungsalgorithmus in Abhängigkeit dieses Verschlüsselungsgeheimnisses (g) und ggf. weiterer, nicht geheimer Parameter eine Zufallszahl (z).

Beispielhaft ist in **Fig. 3** ein typischer Authentikationsvorgang zwischen dem Schlüsselanhänger (1) und dem Garagentoröffner (2) veranschaulicht. Als Startschritt wird die zugehörige Funktionstaste (5) des Schlüsselanhängers (1) betätigt, wodurch der Schlüsselanhänger (1) einen Funktionscode (F_1) in Verbindung mit einem Schlüsselidentitätscode (ID) aussendet, auf dessen Empfang hin sich die Sende-/Empfangseinrichtung (2a) des Garagentoröffners (2) aktiviert. Diese berechnet daraufhin eine Zufallszahl (RND) mittels des DES-Algorithmus in Abhängigkeit von dem abgelegten aktuellen Verschlüsselungsgeheimnis (g), zusätzlich XOR-verknüpft mit einer Konstante (k) von 8 Byte Länge, und einer bisher geltenden Zufallszahl (RND_{alt}). Aufgrund seiner Zufallseigenschaften eignet sich der DES-Algorithmus besonders gut als Pseudozufallsgenerator. Die XOR-Verknüpfung des Verschlüsselungsgeheimnisses (g) mit der Konstanten (k) wirkt sich zusätzlich sicherheitserhöhend aus, so daß mit dem gewählten Algorithmus ein Optimum an Sicherheit, einfacher Logistik und Handhabbarkeit erreicht wird.

Nach Berechnung sendet die Sende-/Empfangseinheit des Garagentoröffners (2) die Zufallszahl (RND) unter optionaler Voraussendung eines zugehörigen Funktionscodes (F_2) als Antwortsignal an den Schlüsselanhänger (1) zurück. Der Schlüsselanhänger (1) chiffriert nach Empfang der Zufallszahl (RND) selbige mit dem DES-Algorithmus unter Verwendung des Verschlüsselungsgeheimnisses (g). Der auf

diese Weise ermittelte Chiffretext (x) wird unter optionaler Voranstellung eines zugehörigen Funktionscodes (F_3) zum Garagentoröffner (2) zurückgesendet. Die Sende-/Empfangseinrichtung des Garagentoröffners (2) bestimmt aus dem Chiffretext (x) unter Verwendung des Verschlüsselungsgeheimnisses (g) durch Anwendung des inversen DES-Algorithmus die enthaltene Klartextinformation und prüft, ob diese der zuvor erzeugten und ausgesendeten Zufallszahl (RND) entspricht. Nur wenn eine Übereinstimmung festgestellt wird, wird auf eine berechtigte Ansteuerung des Garagentoröffners (2) geschlossen, und die Sende-/Empfangseinrichtung (2a) gibt einen zugehörigen Schaltkontakt zur Ansteuerung des Garagentorstellantriebs (2b) frei.

Ein besonderer Vorteil der Fernbedienungseinrichtung liegt darin, daß das für das symmetrische Verschlüsselungsverfahren verwendete Verschlüsselungsgeheimnis (g) in einfacher Weise beliebig oft neu gesetzt werden kann, um eine der ansteuerbaren Funktionseinheiten einem jeweiligen Schlüsselanhänger nutzungsberechtigend zuzuordnen. Hierzu wird ein Verschlüsselungsgeheimnis-Lernvorgang durchgeführt, der nachfolgend anhand der **Fig.** 4 und 5 näher erläutert wird. Die **Fig.** 4 und 5 illustrieren beispielhaft einen solchen Lernvorgang zwischen einem Schlüsselanhänger (1'), der gegenüber demjenigen der **Fig.** 1 und 2 geringfügig modifiziert ist, und dem Garagentoröffner entsprechend **Fig.** 1, von dem in **Fig.** 4 stellvertretend nur ein zugehöriger Wahlschalter (2c) gezeigt ist. Der Wahlschalter (2c) besitzt eine Stellung "Aus", in welcher der Garagentoröffner abgeschaltet ist, eine Stellung "Betrieb", bei der sich der Garagentoröffner im Normalbetrieb zum gesteuerten Öffnen und Schließen des Garagentors befindet, sowie drei Lernmodus-Stellungen "Lernen 1", "Lernen 2" und "Lernen 3", die drei parallelen Lernkanälen entsprechen, über die dem Garagentoröffner drei verschiedene Verschlüsselungsgeheimnisse von drei verschiedenen Schlüsselanhängern zugewiesen werden können, wonach der Garagentoröffner über diese drei Schlüsselanhänger angesteuert werden kann.

Die modifizierten Schlüsselanhänger (1') beinhalten wiederum rückwärtig eine Lernmodus-Funktionstaste (12'), einen Paniktaster (13'), einen Lautsprecher (14') und ein Mikrofon (15') sowie an der Vorderseite ein Display (8'), eine Funktionstaste (5') zur Ansteuerung des Garagentoröffners, eine Funktionstaste (6') zur Ansteuerung des Haustüröffners und eine frei belegbare Funktionstaste (7'), die beispielsweise zum Ein- und Ausschalten eines Hoflichts programmiert werden kann. Bei den modifizierten, als tragbare Fernbedieneinheiten dienenden Schlüsselanhängern (1') ist eine weitere Funktionstaste (16') zur direkten Ansteuerung der Fahrzeugstandheizung anstelle der bei den Schlüsselanhängern (1) gemäß den **Fig.** 1 und 2 vorgesehenen Auswahl über ein Menü angeordnet.

Der in **Fig.** 4 mit seinen Bedienschritten und in **Fig.** 5 im Kommunikationsablauf veranschaulichte Verschlüsselungsgeheimnis-Lernvorgang, mit welchem der Garagentoröffner (2) ein neues Verschlüsselungsgeheimnis (g_{neu}) von einem Schlüsselanhänger (1') lernt, wird wie folgt durchgeführt. Zunächst wird der Lernmodus bei der Sende-/Empfangseinrichtung des Garagentoröffners (2) für den betreffenden Schlüsselanhänger (1') dadurch aktiviert, daß der Wahlschalter (2c) in den zugehörigen Lernkanal, z. B. die Stellung "Lernen 1", gebracht wird. Analog wird der Lernmodus beim betreffenden Schlüsselanhänger (1') durch Drücken der Lernmodus-Funktionstaste (12') aktiviert. Anschließend wird die Funktionstaste (5'), die zu der das neue Verschlüsselungsgeheimnis lernenden Funktionseinheit, hier dem Garagentoröffner (2), gehört, betätigt, woraufhin der Schlüsselanhänger (1') einen entsprechenden Funktionscode (F_4) als Lernmodus-Meldesignal aussendet. Wenn sich die Gegenstelle, d. h. der Garagentoröffner (2), ordnungsgemäß im Lernmodus befindet, bestätigt sie dies auf den Erhalt des vom Schlüsselanhänger (1') ausgesendeten Funktionscodes (F_4) hin durch Absenden eines Lernmodus-Bestätigungssignals in Form eines Antwortfunktionscodes (F_5). Erst auf den Erhalt dieses Bestätigungssignals (F_5) hin erzeugt der Schlüsselanhänger (1') aus einem in ihm anfänglich bei der Produktion implementierten Verschlüsselungsbasisgeheimnis (g_{Basis}) und dem bisher geltenden Verschlüsselungsgeheimnis (g) mittels des DES-Algorithmus ein neues Verschlüsselungsgeheimnis (g_{neu}) als Pseudozufallszahl mit guten Zufallseigenschaften. Bei der erstmaligen Zuweisung eines Verschlüsselungsgeheimnisses wird das anfänglich implementierte Verschlüsselungsbasisgeheimnis (g_{Basis}) als bisheriges Verschlüsselungsgeheimnis verwendet. Durch die Notwendigkeit dieser Bestätigungsmeldung wird ein Entlocken des Verschlüsselungsgeheimnisses aus dem Schlüsselanhänger (1') ohne Gegenstelle unmöglich gemacht. Das Verschlüsselungsgeheimnis wäre in diesem Fall zwar für den betreffenden Angreifer wertlos, da der Garagentoröffner (2) weiterhin nur mit dem bisherigen Verschlüsselungsgeheimnis (g) geöffnet werden könnte, jedoch wäre es bei einer alleinigen Änderung des Verschlüsselungsgeheimnisses im Schlüsselanhänger (1') auch dem berechtigten Benutzer anschließend nicht mehr möglich, den Garagentoröffner (2) mittels des Schlüsselanhängers (1') anzusteuern.

Anschließend wird das neu erzeugte Verschlüsselungsgeheimnis (g_{neu}) zum Garagentoröffner (2) übertragen. Nach Empfang und Abspeicherung des neuen Verschlüsselungsgeheimnisses (g_{neu}) ggf. unter Ersetzung eines bisher zugewiesenen Verschlüsselungsgeheimnisses (g), quittiert die Sende-/Empfangseinrichtung des Garagentoröffners (2) diese ordnungsgemäße Abwicklung durch Aussenden eines entsprechenden Quittierungs-Funktionscodes (F_6). Erst auf Empfang dieses Quittierungssignals (F_6) hin löscht der Schlüsselanhänger (1') das bisher geltende Verschlüsselungsgeheimnis (g), ersetzt es durch das neue Verschlüsselungsgeheimnis (g_{neu}) und gibt dem Benutzer darüber eine optische und/oder akustische Bestätigung über das Display (8') bzw. den Lautsprecher (14'). Es versteht sich, daß bei Bedarf auch alle übrigen, zuvor genannten Bedienhandlungen und Bestätigungen auf dem Display (8') des Schlüsselanhängers (1') dargestellt werden können. Am Wahlschalter (2b) des Garagentoröffners (2) wird dann wieder auf normalen Betrieb umgestellt und der Lernmodus damit deaktiviert, wonach der Garagentoröffner (2) vom Schlüsselanhänger (1') mittels Datenkommunikationsvorgängen angesteuert werden kann, die eine Verschlüsselung basierend auf dem neuen Verschlüsselungsgeheimnis (g_{neu}) beinhalten. Im Schlüsselanhänger (1') wird der Lernbetrieb nach Empfang des Quittierungssignals (F_6) des Garagentoröffners (2) selbsttätig deaktiviert.

Wie ersichtlich, ist es mit dem beschriebenen Verschlüselungsgeheimnis-Lernverfahren in komfortabler Weise möglich, eine tragbare Fernbedieneinheit einerseits und eine über sie ansteuerbare Funktionseinheit andererseits einander nutzungsberechtigend unter beliebig oft wiederholbarer Änderung des Verschlüsselungs geheimnisses zuzuordnen, wobei die Ansteuerung der Funktionseinheit durch die Fernbedieneinheit einen hochsicheren Authentikationsvorgang durch ein symmetrisches Verschlüsselungsverfahren beinhaltet, welches dieses Verschlüsselungsgeheimnis verwendet. Dabei können je nach Anwendungsfall einer Funktionseinheit mehrere nutzungsberechtigende Fernbedieneinheiten und umgekehrt einer Fernbedieneinheit mehrere von ihr ansteuerbare Funktionseinheiten zugewiesen werden.

Patentansprüche

1. Fernbedienungseinrichtung, insbesondere zur Steuerung von kraftfahrzeugbezogenen Einrichtungen, mit

- einer tragbaren Fernbedieneinheit (**1**),
- wenigstens einer über die Fernbedieneinheit ansteuerbaren Funktionseinheit (**2**) und
- einer bidirektionalen Datenkommunikationsstrecke (**17**), über die mittels eines symmetrischen Verschlüsselungsverfahrens codierte Daten zwischen der Fernbedieneinheit und der Funktionseinheit übertragbar sind,

dadurch gekennzeichnet, daß

- die Fernbedieneinheit (1) bei Aktivierung eines Verschlüsselungsgeheimnis-Lernmodus ein Lernmodus-Meldesignal (F_4) abgibt,
- die Funktionseinheit (**2**) im Lernmodus auf den Empfang des Lernmodus-Meldesignals (F_4) hin ein Lernmodus-Bestätigungssignal (F_5) abgibt,
- die Fernbedieneinheit auf Empfang des Lernmodus-Bestätigungssignals hin mittels des Verschlüsselungsalgorithmus des symmetrischen Verschlüsselungsverfahrens in Abhängigkeit eines bisherigen Verschlüsselungsgeheimnisses (g) ein neues Verschlüsselungsgeheimnis (g_{neu}) ermittelt und an die Funktionseinheit sendet,
- die Funktionseinheit nach Empfang des neuen Verschlüsselungsgeheimnisses (g_{neu}) das bisherige Verschlüsselungsgeheimnis (g) durch das neue ersetzt und ein Quittierungssignal (F_6) an die Fernbedieneinheit sendet und
- die Fernbedieneinheit auf Empfang des Quittierungssignals hin das bisherige Verschlüsselungsgeheimnis (g) durch das neue Verschlüsselungsgeheimnis (g_{neu}) ersetzt.

2. Fernbedienungseinrichtung nach Anspruch 1, weiter dadurch gekennzeichnet, daß mit der Fernbedieneinheit (**1**) wenigstens eine fahrzeugseitige Funktionseinheit und wenigstens eine fahrzeugexterne Funktionseinheit (**2**, **3b**) ansteuerbar sind und die Fernbedieneinheit eine optische (**8**) und/oder eine akustische Anzeigevorrichtung (**14**) zum Anzeigen von über die bidirektionale Datenkommunikationsstrecke (**17**) übermittelbaren Informationen aufweist.

3. Fernbedienungseinrichtung nach Anspruch 1 oder 2, weiter dadurch gekennzeichnet, daß die Fernbedieneinheit (**1**) für jede der über sie ansteuerbaren Funktionseinheiten (**2**, **3b**) ein eigenes Verschlüsselungsgeheimnis zur Datenverschlüsselung mittels des Verschlüsselungsalgorithmus verwendet.

4. Fernbedienungseinrichtung nach einem der Ansprüche 1 bis 3, weiter dadurch gekennzeichnet, daß die wenigstens eine Funktionseinheit (**2**) mehrere Lernmodus-Kanäle (Lernen 1, Lernen 2, Lernen 3) zum Lernen jeweils unterschiedlicher Verschlüsselungsgeheimnisse aufweist, die spezifisch jeweils einer von mehreren tragbaren Fernbedieneinheiten (**1**) zugeordnet sind.

5. Fernbedienungseinrichtung nach einem der Ansprüche 1 bis 4, weiter dadurch gekennzeichnet, daß als Verschüsselungsalgorithmus der DES-Algorithmus verwendet wird.

6. Verfahren zur nutzungsberechtigenden, fremdnutzungsgeschützten Zuordnung einer tragbaren Fernbedieneinheit (**1**) zu wenigstens einer über sie ansteuerbaren Funktionseinheit (**2**) mittels Zuweisung eines gemeinsamen, neuen Verschlüsselungsgeheimnisses (g_{neu}) eines zur Authentikation verwendeten symmetrischen Verschlüsselungsverfahrens, gekennzeichnet durch folgende Schritte:

- Aktivieren eines Lernmodus an der Funktionseinheit (**2**) und der Fernbedieneinheit (**1'**) und Senden eines Lernmodus-Meldesignals (F_4) von der Fernbedieneinheit zur Funktionseinheit,
- Senden eines Lernmodus-Bestätigungssignals (F_5) von der Funktionseinheit zur Fernbedieneinheit auf den Empfang des Lernmodus-Meldesignals (F_4) hin,
- Berechnen des neuen Verschlüsselungsgeheimnisses (g_{neu}) mittels des Verschlüsselungsalgorithmus des symmetrischen Verschlüsselungsverfahrens in Abhängigkeit von einem Verschlüsselungsbasisgeheimnis (g_{Basis}) und des bisherigen Verschlüsselungsgeheimnisses (g) und Übertragung desselben an die Funktionseinheit durch die Fernbedieneinheit auf den Empfang des Lernmodus-Bestätigungsignals (F_5) hin,
- Ersetzen des bisherigen Verschlüsselungsgeheimnisses (g) durch das empfangene, neue Verschlüsselungsgeheimnis (g_{neu}) in der Funktionseinheit und Absenden eines Quittierungssignals (F_6) durch die Funktionseinheit und
- Ersetzen des bisherigen Verschlüsselungsgeheimnisses (g) durch das neue Verschlüsselungsgeheimnis (g_{neu}) in der Fernbedieneinheit auf den Empfang des Quittierungssignals (F_6) hin.

7. Verfahren nach Anspruch 6, weiter dadurch gekennzeichnet, daß für jede von mehreren, über die Fernbedieneinheit ansteuerbaren Funktionseinheiten ein eigenes Verschlüsselungsgeheimnis zur Datenverschlüsselung mittels des Verschlüsselungsalgorithmus verwendet wird.

8. Verfahren nach Anspruch 6 oder 7, weiter dadurch gekennzeichnet, daß der wenigstens einen Funktionseinheit mehrere Lernmodus-Kanäle (Lernen 1, Lernen 2, Lernen 3) zum Lernen jeweils unterschiedlicher Verschlüsselungsgeheimnisse zugewiesen werden, die spezifisch jeweils einer von mehreren tragbaren Fernbedieneinheiten zugeordnet sind.

9. Verfahren nach einem der Ansprüche 6 bis 8, weiter dadurch gekennzeichnet, daß als Verschlüsselungsalgorithmus der DES-Algorithmus verwendet wird.

Hierzu 4 Seite(n) Zeichnungen

Numm r: DE 196 07 017 C2
Int. Cl.[7]: H 04 Q 9/00
Veröffentlichungstag: 29. Juni 2000

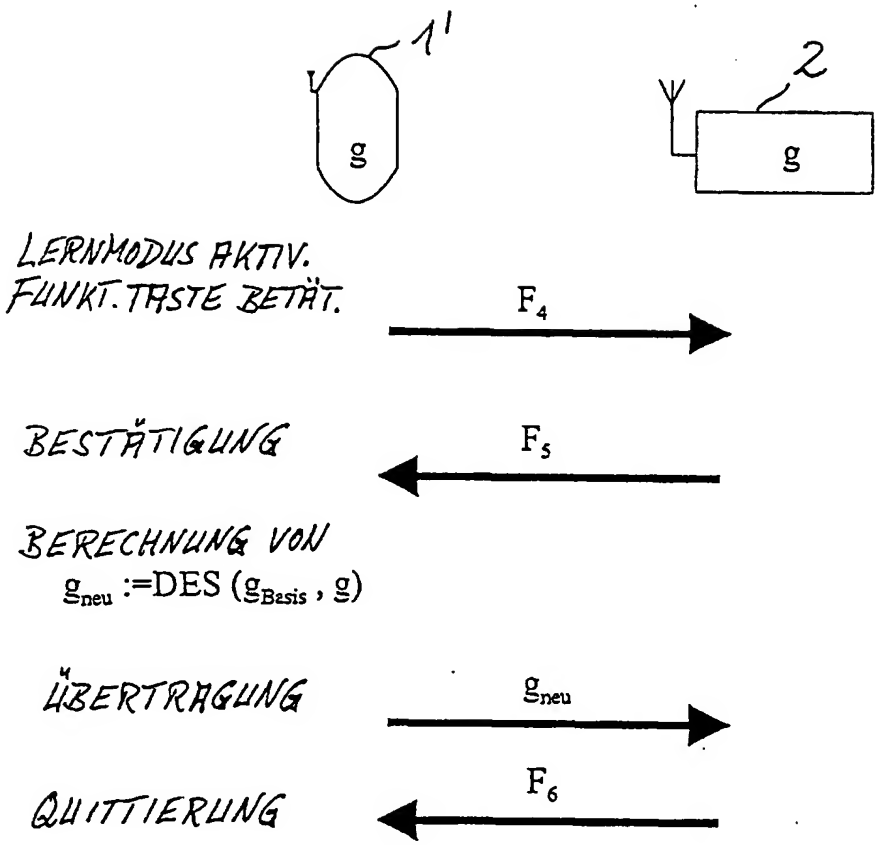


Fig. 5

Numm r: DE 196 07 017 C2
Int. Cl.[7]: H 04 Q 9/00
Veröffentlichungstag: 29. Juni 2000

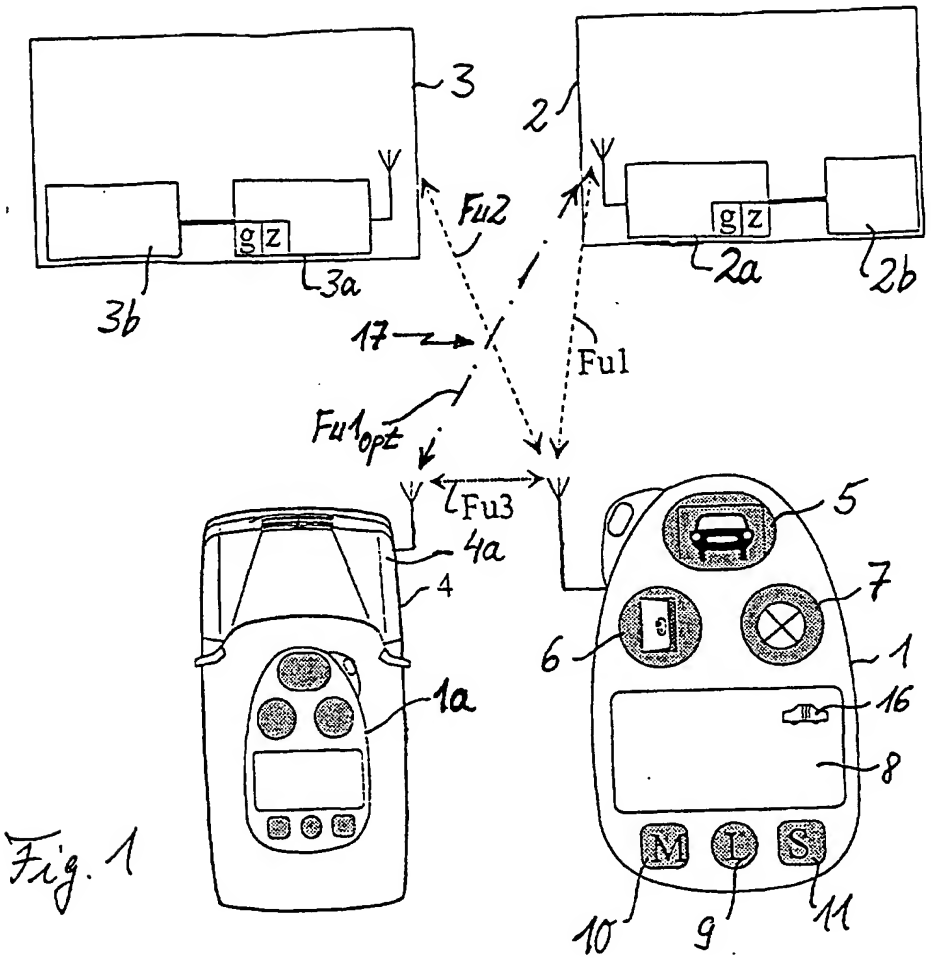


Fig. 1

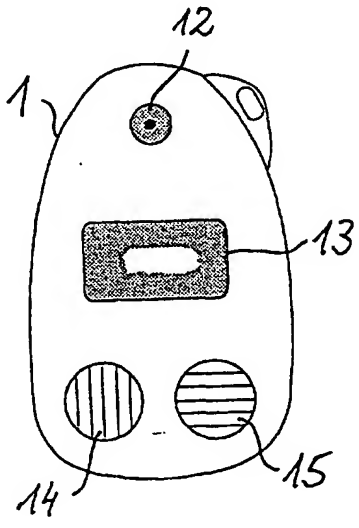


Fig. 2

Numm r: DE 196 07 017 C2
Int. Cl.[7]: H 04 Q 9/00
Veröffentlichungstag: 29. Juni 2000

1. Start — F_1 / ID →

2. Berechnung — RND :=DES((g XOR k), RND_{alt})

3. Antwort — ← F_2 / RND

4. Berechnung
x := DES (g, RND)

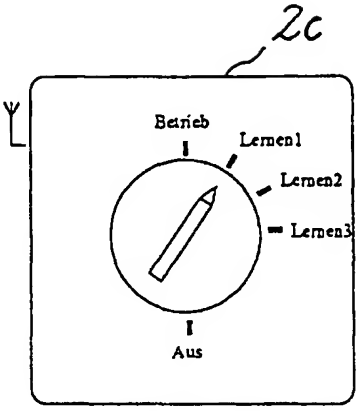
5. Authentikation — F_3 / x →

6. Prüfung — $RND = DES^{-1}(g, x)$?

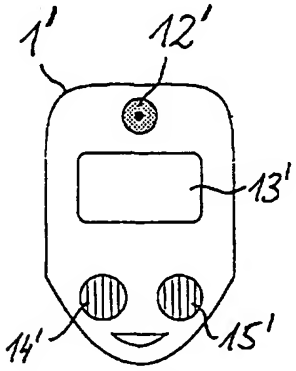
7. Freigabe des Schaltkontaktes für den Garagentoröffner

Fig. 3

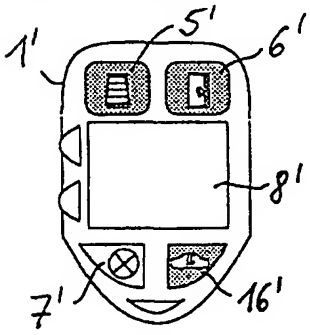
Nummer: DE 196 07 017 C2
Int. Cl.[7]: H 04 Q 9/00
Veröffentlichungstag: 29. Juni 2000



AN GAR. TORÖFFNER
LERNMODUS AKTIVIEREN

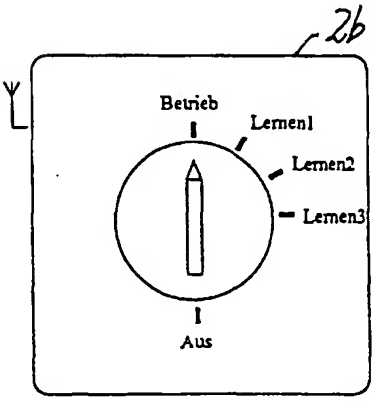


AN SCHLÜSSELANHÄNGER
LERNMODUS AKTIVIEREN



ZUGEHÖRIGE FUNKTIONS-
TASTE BETÄTIGEN

BESTÄTIGUNGSMELDUNG
ABWARTEN



AN GAR. TORÖFFNER
LERNMODUS DEAKTIVIEREN

Fig. 4